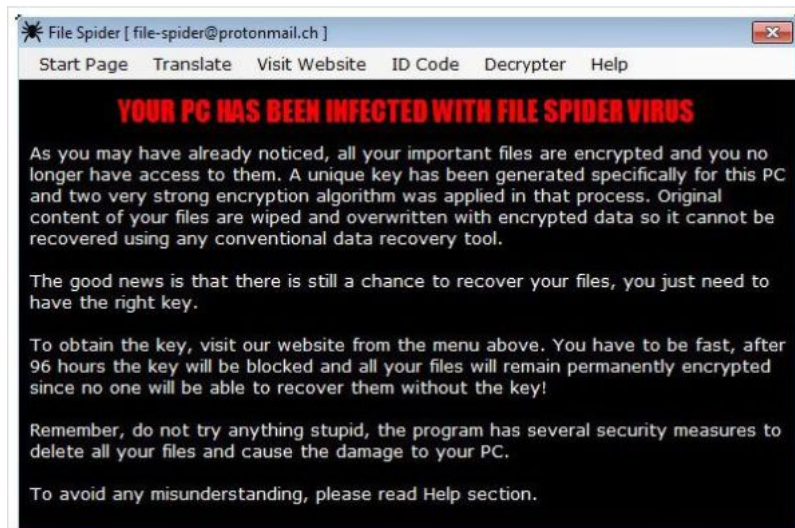


Spider PC Dateien Virus - Ransomware erpresst Europa

13.12.2017, 09:38 | IT, New Media & Software

Pressemitteilung von: *Virus-Entferner*



..spider Dateiverschlüsselung

File Spider ist ein Ransomware-Virus, der von Malware-Sicherheitsforscher Lawrence Abrams entdeckt wurde. Es wird mithilfe von Spam-E-Mails mit schädlichen Anhängen (MS Office-Dokumente) verteilt, die einen Makrobefehl zum Herunterladen und Ausführen von Malware ausführen. Entwickler richten sich hauptsächlich an Nutzer aus Serbien, Bosnien und Herzegowina und Kroatien. Unmittelbar nach der Infiltration verschlüsselt File Spider die meisten gespeicherten Dateien und hängt Dateinamen mit der Erweiterung ".spider" an (z. B. wird "sample.jpg" zu "sample.jpg.spider"). Von diesem Punkt werden Dateien unbrauchbar. Sobald die Dateien verschlüsselt sind, führt File Spider die Datei "dec.exe" aus (wird vom Anhang heruntergeladen und im Ordner "% AppData% \ Spider" gespeichert). Darüber hinaus erstellt es zwei Verknüpfungen: "WIE ENTSTEHEN FILES.url" (in jedem vorhandenen Ordner platziert und führt zu einem "wie Entschlüsseln" Online-Video-Tutorial) und "DECRYPTER.url" (auf dem Desktop platziert, und das öffnet die Datei "dec.exe").

Das Popup-Fenster enthält eine Nachricht, die die Opfer über die Verschlüsselung informiert und sie anweist, was als nächstes zu tun ist. Um Dateien wiederherzustellen, müssen Benutzer zuerst die Website von File Spider besuchen und ein Lösegeld bezahlen. Die Nachricht besagt, dass für die Entschlüsselung ein eindeutiger Schlüssel erforderlich ist. Leider sind diese Informationen korrekt. File Spider verwendet die AES-128-Kryptographie und somit ist es unmöglich, Dateien wiederherzustellen, ohne dass ein Schlüssel für jedes Opfer eindeutig generiert wird. Zusätzlich wird der Primärschlüssel mit dem RSA-Algorithmus (der einen zweiten Schlüssel erzeugt) verschlüsselt, wodurch die Dinge noch komplizierter werden. Cyber-Kriminelle speichern diese Schlüssel auf einem Remote-Server, und Benutzer werden aufgefordert, 0,00725 Bitcoin (im Gegenwert von etwa 120 Euro) dafür zu bezahlen. Die Botschaft besagt auch, dass die Opfer vier Tage (genau 96 Stunden) Zeit haben, die Zahlung zu leisten. Nach diesem Zeitraum werden die Schlüssel dauerhaft blockiert / gelöscht und das Wiederherstellen von Dateien wird unmöglich. Trotz dieser Bedrohungen und Forderungen können Cyber-Kriminelle nicht vertraut werden. Die Forschung zeigt, dass diese Menschen Opfer oft ignorieren, sobald Lösegelder bezahlt werden. Wenn Sie zahlen, besteht eine hohe Wahrscheinlichkeit, dass Sie betrogen werden und kein positives Ergebnis erhalten. Neben dem Verlust Ihres Geldes unterstützen Sie auch böartige Geschäfte von Cyberkriminellen. Daher raten wir Ihnen dringend, alle Zahlungsanfragen zu ignorieren. Leider gibt es keine Tools, mit denen Dateien wiederhergestellt werden können, die mit dieser Ransomware verschlüsselt wurden. Die einzige Lösung besteht darin, Ihre Dateien / Ihr System aus einem Backup wiederherzustellen.

<https://www.virus-entferner.de/spider-ransomware-datei-virus-entfernen/>

Ihr Virus-Entferner Team

Portrait

Das Projekt Virus-Entferner macht es sich zur Aufgabe Computernutzer über Ransomware, Schadsoftware, Adware und andere im Internet kursierende gefährliche Programme zu informieren. Virus-Entferner ist eine grosse Quelle für sicherheitsorientierte Informationen, die für das Verhindern oder Entfernen von Viren wesentlich sind. Wir bieten klare und professionell geschriebene Parasitenbeschreibungen, ausführliche Entfernungsanweisungen, Beurteilungen für Anti-Spyware, Antivirensoftware und vieles mehr.

News-ID: 985152 • Views: 2260 (Stand: 10.05.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/985152/Spider-PC-Dateien-Virus-Ransomware-erpresst-Europa.html>